UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Premises located at 8114 NE 145th Street, Kenmore Washington, 98028 et al., as more fully described in Attachments A-1 and A-2	)	Case No. MJ21-417

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachments A-1 and A-2, which is incorporated herein by reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C § 875(c)	Threats Made Using Interstate Commerce

The application is based on these facts:

✓ See Affidavit of FBI Special Agent Matthew Morgan, continued on the attached sheet.

☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☑ by reliable electronic means; or: ☐ telephonically recorded.

Applicant's signature

Matthew Morgan, FBI Special Agent

Printed name and title

◯ The foregoing affidavit was sworn to before me and signed in my presence, or
◉ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 07/17/2021

Judge's signature

City and state: Seattle, Washington

Michelle L. Peterson, United States Magistrate Judge

Printed name and title

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, Matthew Morgan, having been duly sworn, state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed since December 6, 2020. I am presently assigned to work domestic terrorism threats which have a nexus in the state of Washington.

2. I make this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises located at **8114 NE 145th Street, Kenmore, Washington 98028** (hereinafter, the "SUBJECT PREMISES"), as more fully described in Attachment A-1 to the Affidavit, for the property and items described in Attachment B to this Affidavit, and for a warrant to search the person of Coen Davis OWSLEY, as more fully described in Attachment A-2 to this Affidavit, for the property and items described in Attachment B to this Affidavit, as well as any digital devices or other electronic storage media located in either location.

3. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; review of documents and records related to this investigation; and information gained through my training and experience.

4. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits and instrumentalities of violations of Title 18, United States Code, Section 875(c) (Threats Made Using Interstate Communications) will be found at the SUBJECT PREMISES and on OWSLEY's person.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

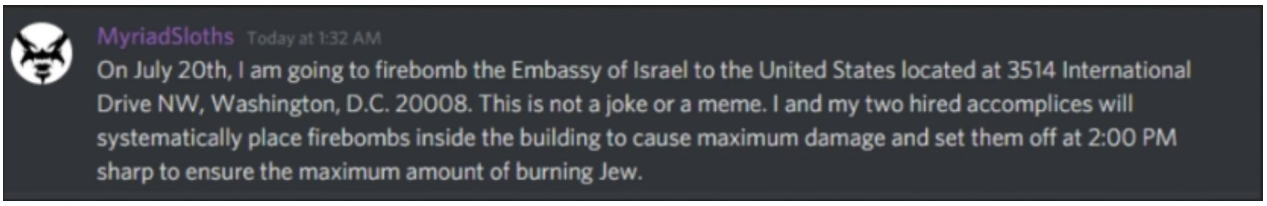
THE INVESTIGATION

The Initial Tip

5. On or around July 6, 2021, the FBI's National Threat Operations Center received an anonymous tip that an individual with the username **MyriadSloths#4248** (the "SUBJECT USERNAME") had threatened to carry out a coordinated attack against the Israeli Embassy located in Washington, D.C. The threat was made in a private Discord chat, which has approximately 104 members.

6. Based on my training and experience, I know that Discord is a US-based proprietary freeware voice over the Internet protocol ("VOIP") application that specializes in text, video and audio communication. Discord was initially designed for the gaming community but is now widely used by academia, the business community, and groups with common interests. Discord chat channels or private groups are known as "servers." Users can share their screen, post images, text, voice chat or send direct messages to other users within a server. Servers are controlled by one or more administrators who manage membership and content. Servers are organized by specific topics of interest using sub-channels which an administrator can restrict by role. Additionally, administrators may control access to a server by implementing vetting procedures prior to admittance.

7. The anonymous tipster provided the below screenshot of the SUBJECT USERNAME'S threat, which states, "On July 20th, I am going to firebomb the Embassy of Israel to the United States located at 3541 International Drive NW, Washington, D.C. 20008. This is not a joke or meme. I and my two hired accomplices will systemically place firebombs inside the building to cause maximum damage and set them off at 2:00 PM sharp to ensure the maximum amount of burning Jew."



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

8. Additionally, the anonymous tipster also wrote that, while he/she did not personally know the SUBJECT USERNAME, he/she had observe the SUBJECT USERNAME for over a year writing anti-Semitic messages, using Nazi and anti-Semitic symbolism and language, and espousing violence towards Jews. The tipster further stated that he/she had previously reported the SUBJECT USERNAME to Discord moderators, and Discord moderators had responded by deleting the offending messages. Finally, the tipster noted that the SUBJECT USERNAME associated with several other individuals who shared similar views and posted similar content.

Law Enforcement's Response

9. In response to this tip, law enforcement took numerous steps to quickly identify the individual using the SUBJECT USERNAME.

10. Records obtained from Discord revealed that the email addressed registered to the SUBJECT USERNAME was **coendowsley@gmail.com** ("EMAIL ACCOUNT 1") with the registration IP address as **73.181.251.9** (the "REGISTERED IP ADDRESS"). IP address logins for the SUBJECT USERNAME included the REGISTERED IP ADDRESS, 172.56.42.64, 172.56.42.211, 172.56.42.135, 172.56.42.227, 172.56.42.5, 172.56.42.207, 172.56.42.171, 172.56.42.184, 172.56.42.85, 172.56.42.92.

11. Investigators also identified other usernames associated with the SUBJECT USERNAME on Discord and other social media platforms, including "MyriadSloths#1514," "MyriadSloths," "neoccoen," and "The Black Sun." "The Black Sun" is regularly used by neo-Nazi groups in place of the more recognizable swastika. In searching various social media sites, investigators also uncovered a video gaming account with the username "MyriadSloths" that was linked to another username "kill women."

12. Records obtained from Google revealed that OWSLEY is the subscriber for EMAIL ACCOUNT 1. Furthermore, Google provided a linked telephone number (425-780-1977) and linked cellphone (Samsung model SM-G973U with IMEI 356142110240223). Other linked usernames include MyriadSloths@gmail.com, CoenTheOwsley@gmail.com, Neoc139@gmail.com, alienboy.x@gmail.com,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

myriadmetanoia@gmail.com, coendowsley@gmail.com. These various emails match the previously known usernames and handles associated with the SUBJECT USERNAME that posted the threat under investigation on Discord.

13. Based on evidence obtained to date, investigators have also learned that the REGISTERED IP ADDRESS is the most frequently utilized IP address the SUBJECT USERNAME or its linked accounts to log into Discord. The REGISTERED IP ADDRESS was also the IP address used for the SUBJECT USERNAME or its linked accounts on Discord near the time that the threat was made.

14. Moreover, records from the internet service provider Comcast confirmed that the REGISTERED IP ADDRESS resolved to the SUBJECT PREMISES.

15. I believe that there is probable cause to believe that the communications at issue were sent from the SUBJECT PREMISES or other locations within the State of Washington and crossed state line as Discord's servers are all located outside the State of Washington.

Surveillance of the SUBJECT PREMISES

16. Department of Licensing and other government records show OWSLEY's listed address is the SUBJECT PREMISES. According to records, he resides at the SUBJECT PREMISES with his parents and younger brother.

17. On July 16, 2021, law enforcement officers observed OWSLEY at the SUBJECT PREMISES.

Accessing Samsung Galaxy Devices

18. I know from my training and experience, as well as information found in publicly available materials including those published by Samsung, that some models of Samsung devices offer their users the ability to unlock the devices via the use of facial recognition in lieu of a numeric or alphanumeric passcode or password.

19. I further know that time will be of the essence in securing any electronic communications, including Discord messages, that are seized from OWSLEY. Moreover, I know that messages from Discord may be remotely deleted.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

20. Due to the foregoing, I respectfully request that the Court authorize law enforcement to present the face of OWSLEY to the camera of Samsung Galaxy devices for the purpose of attempting to unlock the device via facial recognition in order to execute the searches and/or seizures authorized by the requested warrants.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

21. As described above and in Attachment B, this application seeks permission to search for evidence, fruits and instrumentalities that might be found at the SUBJECT PREMISES or on OWSLEY's person, in whatever form they are found. One form in which the evidence and/or instrumentalities might be found is data stored on digital devices[1] such as computer hard drives or other electronic storage media.[2] Thus, the warrant applied for would authorize the seizure of digital devices or other electronic storage media or, potentially, the copying of electronically stored information from digital devices or other electronic storage media, all under Rule 41(e)(2)(B).

22. *Probable cause.* Based upon my review of the evidence gathered in this investigation, my review of data and records, information received from other agents and computer forensics examiners, and my training and experience, I submit that if a digital device or other electronic storage media is found at the SUBJECT PREMISES or on OWSLEY's person, there is probable cause to believe that evidence and/or instrumentalities of the crimes of Title 18, United States Code, Section 875(c) (Threats

---

[1] "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

[2] Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Made Using Interstate Communications) will be stored on those digital devices or other electronic storage media. Based on my training and experience, I believe digital devices or other electronic storage media were used to participate in the private Discord chat in which OWSLEY threatened violence against the Israeli Embassy. I also believe that OWSLEY is utilizing aforementioned devices and media to communicate with any co-conspirators referenced in the threat. There is, therefore, probable cause to believe that evidence, fruits, and instrumentalities of the crimes of Title 18, United States Code, Section 875(c) (Threats Made Using Interstate Communications) exists and will be found on digital device or other electronic storage media at the SUBJECT PREMISES or on OWSLEY's person for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be preserved (and consequently also then recovered) for months or even years after they have been downloaded onto a storage medium, deleted, or accessed or viewed via the Internet. Electronic files downloaded to a digital device or other electronic storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a digital device or other electronic storage media, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device or other electronic storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

23. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how digital devices or other electronic storage media were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any digital devices or other electronic storage media located at the SUBJECT PREMISES and OWSLEY's person because:

a. Stored data can provide evidence of a file that was once on the digital device or other electronic storage media but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the digital device or other electronic storage media that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the history of connections to other computers, the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device or other electronic storage media was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

c. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner and/or others with direct physical access to the computer. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation.

d. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user.

e. Furthermore, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

f. A person with appropriate familiarity with how a digital device or other electronic storage media works can, after examining this forensic evidence in its proper context, draw conclusions about how the digital device or other electronic storage media were used, the purpose of their use, who used them, and when.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

g. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device or other electronic storage media that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

h. Further, in finding evidence of how a digital device or other electronic storage media was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

DIGITAL DEVICES AS INSTRUMENTALITIES OF THE CRIMES

24. Based on my training and experience, I know that, in order to access Discord, a user needs to utilize either a computer or mobile device with internet access. This is the only way in which OWSLEY could have posted the threat to firebomb the Israeli Embassy in Washington, D.C.

REQUEST FOR AUTHORITY TO CONDUCT OFF-SITE SEARCH OF TARGET COMPUTERS

25. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of premises for information that might be stored on digital devices or other electronic storage media often requires the seizure of the physical items and later off-site review consistent with the warrant. In lieu of removing all of these items from the premises, it is sometimes possible to make an image copy of the data on the digital devices or other electronic storage media, onsite. Generally speaking, imaging is the taking of a complete electronic picture of the device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the item, and to prevent the loss of the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination*. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine the respective digital device and/or electronic storage media to obtain evidence. Computer hard drives, digital devices and electronic storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements*. Digital devices or other electronic storage media can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the items off-site and reviewing them in a controlled environment will allow examination with the proper tools and knowledge.

c. *Variety of forms of electronic media*. Records sought under this warrant could be stored in a variety of electronic storage media formats and on a variety of digital devices that may require off-site reviewing with specialized forensic tools.

SEARCH TECHNIQUES

26. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for will permit seizing, imaging, or otherwise copying digital devices or other electronic storage media that reasonably appear capable of containing some or all of the data or items that fall within the scope of Attachment B to this Affidavit, and will specifically authorize a later review of the media or information consistent with the warrant.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

27. Because several people share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain digital devices or other electronic storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If agents conducting the search nonetheless determine that it is possible that the things described in this warrant could be found on those computers, this application seeks permission to search and if necessary to seize those computers as well. It may be impossible to determine, on scene, which computers contain the things described in this warrant.

28. Consistent with the above, I hereby request the Court's permission to seize and/or obtain a forensic image of digital devices or other electronic storage media that reasonably appear capable of containing data or items that fall within the scope of Attachment B to this Affidavit, and to conduct off-site searches of the digital devices or other electronic storage media and/or forensic images, using the following procedures:

A. Processing the Search Sites and Securing the Data.

a. Upon securing the physical search site, the search team will conduct an initial review of any digital devices or other electronic storage media located at the SUBJECT PREMISES described in Attachment A-1 and on OWSLEY's person as described in Attachment A-2 that are capable of containing data or items that fall within the scope of Attachment B to this Affidavit, to determine if it is possible to secure the data contained on these devices onsite in a reasonable amount of time and without jeopardizing the ability to accurately preserve the data.

b. In order to examine the electronically stored information ("ESI") in a forensically sound manner, law enforcement personnel with appropriate expertise will attempt to produce a complete forensic image, if possible and appropriate, of any digital device or other electronic storage media that is capable of containing data or items that fall within the scope of Attachment B to this Affidavit.[1]

[1] The purpose of using specially trained computer forensic examiners to conduct the imaging of digital devices or other electronic storage media is to ensure the integrity of the evidence and to follow proper, forensically sound, scientific procedures. When the investigative agent is a trained computer forensic examiner, it is not always necessary to separate these duties. Computer forensic examiners often work closely with investigative

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

c. A forensic image may be created of either a physical drive or a logical drive. A physical drive is the actual physical hard drive that may be found in a typical computer. When law enforcement creates a forensic image of a physical drive, the image will contain every bit and byte on the physical drive. A logical drive, also known as a partition, is a dedicated area on a physical drive that may have a drive letter assigned (for example the c: and d: drives on a computer that actually contains only one physical hard drive). Therefore, creating an image of a logical drive does not include every bit and byte on the physical drive. Law enforcement will only create an image of physical or logical drives physically present on or within the subject device. Creating an image of the devices located at the search locations described in Attachments A-1 and A-2 will not result in access to any data physically located elsewhere. However, digital devices or other electronic storage media at the search locations described in Attachments A-1 and A-2 that have previously connected to devices at other locations may contain data from those other locations.

d. If based on their training and experience, and the resources available to them at the search site, the search team determines it is not practical to make an on-site image within a reasonable amount of time and without jeopardizing the ability to accurately preserve the data, then the digital devices or other electronic storage media will be seized and transported to an appropriate law enforcement laboratory to be forensically imaged and reviewed.

B. Searching the Forensic Images.

a. Searching the forensic images for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement may need to conduct more extensive searches to locate evidence that falls within the scope of the warrant. The

---

personnel to assist investigators in their search for digital evidence. Computer forensic examiners are needed because they generally have technological expertise that investigative agents do not possess. Computer forensic examiners, however, often lack the factual and investigative expertise that an investigative agent may possess on any given case. Therefore, it is often important that computer forensic examiners and investigative personnel work closely together.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this Affidavit. Those techniques, however, may necessarily expose many or all parts of a hard drive to human inspection in order to determine whether it contains evidence described by the warrant.

///

///

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

CONCLUSION

29. Based on the foregoing, I believe there is probable cause to search the above-described SUBJECT PREMISES, as further described in Attachment A-1, and the person of Coen Davis OWSLEY, as further described in Attachment A-2, for evidence, fruits and instrumentalities, as further described in Attachment B, of crimes committed by OWSLEY and his co-conspirators, specifically in violation of Title 18, United States Code, Section 875(c) (Threats Made Using Interstate Communications).

MATTHEW MORGAN, Affiant
Special Agent
Federal Bureau of Investigation

The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone on this 17th day of July, 2021.

MICHELLE L. PETERSON
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-1

Place to be Searched

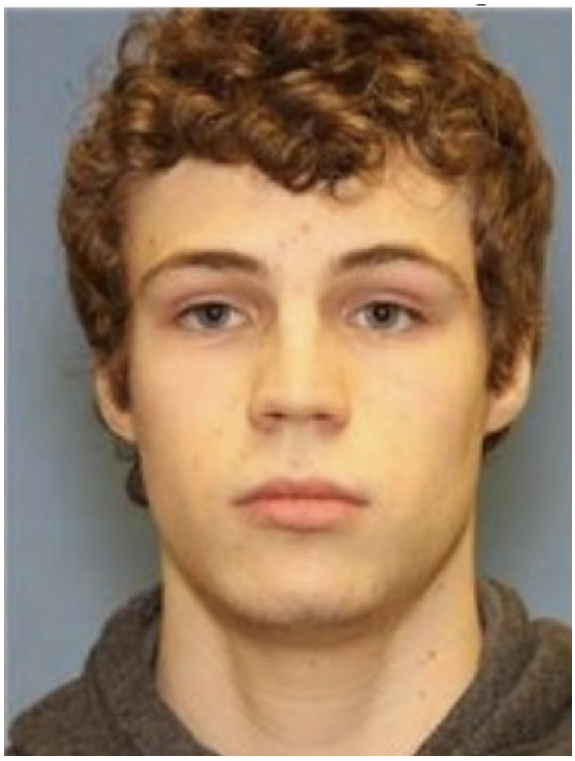
The property to be searched is 8114 NE 145th Street, Kenmore, Washington 98028. The residence is a blue, two-story house with white trim that is located on the northside of NE 145 Street.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-2

Person to be Searched

This warrant authorizes the search of the person of Coen Davis OWSLEY, the person associated with 8114 NE 145th Street, Kenmore, Washington 98028, and any digital device or other electronic storage media found on his person.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B
Items to be Seized

This warrant authorizes the government to search for the following evidence, fruits and/or instrumentalities of Title 18, United States Code, Section 875(c) (Threats Made Using Interstate Communications) for the time period January 1, 2020 through the present, whether recorded on paper or stored electronically on computers and related peripheral devices:

1. Samsung cellular telephone identified as model SM-G973U, IMEI 356142110240223, and/or linked to telephone number (425) 780-1977 (hereinafter, "SAMSUNG CELLPHONE")
2. Other digital devices[1] or other electronic storage media[2] and/or their components devices (collectively, "Other Electronic Devices") may be seized and searched for the following items:
   a. Assigned number and identifying telephone serial number (ESN, MIN, IMSI, or IMEI);
   b. Stored list of recent received, sent, and missed calls;
   c. Stored contact information;
   d. Stored photographs and videos related to the aforementioned crime under investigation, including any embedded GPS data associated with these photographs and videos;
   e. Stored emails, including their contents, related to the aforementioned crimes under investigation or that may show the user of the phone and/or co-conspirators;
   f. Stored text messages, as well as any messages in any internet messaging apps, including but not limited to Discord, Facebook Messenger, WhatsApp, and similar messaging applications, related to the

[1] "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

[2] "Electronic storage media" is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

aforementioned crimes under investigation or that may show the user of the phone and/or co-conspirators;

g. Stored documents, notes, and files that contain passwords or encryption keys;

h. Any records or information related to the use of usernames "MyriadSloths#4248" and its variations, "neoccoen," and "The Black Sun."

3. For Other Electronic Devices, if law enforcement can reasonably determine that Coen Davis OWSLEY neither owns nor has access to a particular digital device or electronic storage media, this warrant DOES NOT authorize its seizure or search.

4. For any digital device or other electronic storage media upon which electronically stored information that is called for by this warrant may be contained, or that may contain things otherwise called for by this warrant:

a. Evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. Evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. Evidence of the lack of such malicious software;

d. Evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

e. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

f. Evidence of the times the digital device or other electronic storage media was used;

g. Passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;

h. Documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media; and

i. Contextual information necessary to understand the evidence described in herein.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

5. Records of or information about the use of Internet Protocol address **73.181.251.8** to communicate with Comcast or Discord including:

   a. Routers, modems, and network equipment used to connect computers to the Internet;

   b. Records of Internet Protocol addresses used; and

   c. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses

During the execution of the warrant, law enforcement personnel are authorized to present the face of Coen Davis OWSLEY to the camera of SAMSUNG CELLPHONE to be searched for the purpose of attempting to unlock the device in order to search and seize items as authorized by this warrant.

THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970